Journal of Number Theory 131 (2011) 936–958

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Special Issue: Elliptic Curve Cryptography

Computing genus 2 curves from invariants on the Hilbert moduli space

Kristin Lauter [a,*], Tonghai Yang [b]

[a] Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
[b] Department of Mathematics, University of Wisconsin Madison, Van Vleck Hall, Madison, WI 53706, USA

ARTICLE INFO

Article history:
Received 19 May 2010
Accepted 19 May 2010
Available online 19 August 2010
Communicated by N. Koblitz and V.S. Miller

Keywords:
Hyperelliptic genus 2 curve
Complex multiplication
Hilbert modular forms
Public-key cryptography

MSC:
11G15
11F41
14K22

ABSTRACT

We give a new method for generating genus 2 curves over a finite field with a given number of points on the Jacobian of the curve. We define two new invariants for genus 2 curves as values of modular functions on the Hilbert moduli space and show how to compute them. We relate them to the usual three Igusa invariants on the Siegel moduli space and give an algorithm to construct curves using these new invariants. Our approach simplifies the complex analytic method for computing genus 2 curves for cryptography and reduces the amount of computation required.

1. Introduction

Genus 2 curves over finite fields are an important source of groups for use in cryptography, since there are no known subexponential algorithms for the discrete logarithm problem on the Jacobian of a general genus 2 curve over a finite field. Compared to elliptic curves, Jacobians of genus 2 curves offer comparable security levels over a field of half the bit size, since the group size of the Jacobian of a genus 2 curve over a finite field $\mathbb{F}_p$ is roughly p^2, as opposed to size p for elliptic curves. The recent advent and prevalence of 64-bit machines has made higher genus curves seem more attractive, as the possibility of field elements which fit into a single word nears, thereby improving the efficiency of field operations.

* Corresponding author.
E-mail addresses: klauter@microsoft.com (K. Lauter), thyang@math.wisc.edu (T. Yang).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.05.012

However, to avoid Pohlig–Hellman attacks and to obtain optimal security over a field of a given bit-size, it is necessary to construct Jacobians whose order is prime, or at worst has a very small cofactor. Since point-counting methods for determining the order of the Jacobian of a random genus 2 curve over a finite field are not practical when the characteristic is large, the only practical solution is to construct curves which have a Jacobian with a given group size. Also, pairings on Jacobians of genus 2 curves provide an alternative for implementing pairing-based cryptosystems. When generating pairing-friendly curves, there are additional divisibility constraints to be satisfied and selecting curves via construction is the only practical option. Constructing genus 2 curves over prime fields of cryptographic size so that the group size is a given prime order is a great challenge, and the only currently known solution is to use deep mathematical methods based on the theory of Complex Multiplication (CM).

For the last 15 years, genus 2 curves with CM have been constructed by determining the Bolza–Clebsch–Igusa invariants of the curve. Clebsch defined the invariants of binary sextics in the 1880s and Bolza showed that they were related to modular invariants of the Jacobian of the curve viewed as a complex torus; much later Igusa [Ig1] defined a complete set of invariants which works in all characteristics and which can be computed as values of certain Siegel modular functions on the Siegel upper half plane. The moduli space of genus 2 curves is 3-dimensional and so three invariants are needed to specify a curve up to isomorphism over an algebraically closed field. To compute these Igusa invariants, Spallek [Sp] determined a collection of representatives for isomorphism classes of polarized abelian surfaces with CM by a given field. Determining this set was complicated, and a complete set of representatives in general was not determined until the recent work of Streng [St]. In [We], Weng gave an algorithm for computing the minimal polynomials of Igusa invariants by evaluating Siegel modular forms to very high precision in order to recognize the coefficients of the minimal polynomials as rational numbers. Unfortunately, the large number of floating point multiplications performed in the computation causes loss of precision and makes the algorithm hard to analyze [St].

In this paper we present a new approach to computing genus 2 curves by defining a different set of invariants which are simpler than Igusa invariants. We fix a real quadratic field F and consider the Hilbert moduli space of principally polarized abelian surfaces with real multiplication by $\mathcal{O}_F$. The forgetful functor gives a map to the Siegel moduli space of principally polarized abelian surfaces. We study the two generators of the function field of the Hilbert moduli space as given by Gundlach [Gu], and show how they can be used to generate genus 2 curves with a Jacobian of given order. We compute the pullback of the Igusa functions to the Hilbert moduli space and express them in terms of our new invariants.

The algorithm we present has at least three advantages over the complex analytic method which generates genus 2 curves from Igusa invariants. First, there are only two invariants to be computed as values of modular forms, not three. Second, the description of CM points on the Hilbert moduli space is simpler than the description of CM points in terms of period matrices on the Siegel moduli space. Finally, the modular forms we evaluate in order to compute invariants on the Hilbert moduli space are exponential functions in two variables, instead of three. This leads to fewer evaluations of exponential functions and fewer high-precision floating point multiplications. In essence, our method takes advantage of the beautiful relationship between invariants on the Hilbert and Siegel moduli spaces. It relies on the explicit description of the pullback map which can be used to express the more complicated modular functions on the Siegel moduli space in terms of simpler modular functions on the Hilbert moduli space. Throughout this paper we will assume $F = Q(\sqrt{5})$, but the method will also work for some other real quadratic fields $F = Q(\sqrt{D})$, whose associated Hilbert modular surface are rational surfaces.

In Section 2, we give background on Igusa invariants and the CM method for generating genus 2 curves. In Section 3, we describe the map between the Hilbert and Siegel spaces. In Section 4, we compute the Hilbert Eisenstein series, define the new invariants, and compute the pullback of the Igusa functions in terms of the new invariants. In Section 5, we show how to compute CM points on the Hilbert moduli space and give our algorithm for computing genus 2 curves. In Section 6, we give two concrete examples of how the algorithm works. Appendix A gives unoptimized code for computing the new invariants and explains Mestre's algorithm for generating genus 2 curves from their invariants.

2. Generating genus 2 curves with CM

2.1. Number of points on the Jacobian

For an ordinary genus 2 curve C over a finite prime field $\mathbb{F}_p$, let $N_1 = \#C(\mathbb{F}_p)$ and $N_2 = \#C(\mathbb{F}_{p^2})$. Then

$$\#J(C)(\mathbb{F}_p) = N = \left(N_1^2 + N_2\right)/2 - p. \tag{2.1}$$

To find a curve C over $\mathbb{F}_p$ such that $\#J(C) = N$, first find N_1 and N_2 in the Hasse–Weil intervals for $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ satisfying relation (2.1), if they exist. Next, set $N_1 = p+1-s_1$ and $N_2 = p^2+1+2s_2-s_1^2$. Then the quartic polynomial $h(t) = t^4 - s_1t^3 + s_2t^2 - ps_1t + p^2$ is the Weil polynomial of a genus 2 curve as long as the exceptional cases listed in [HNR, Theorem 1.2] are avoided. Under those conditions, the Jacobian of the curve has endomorphism ring equal to an order in the quartic CM field $K = \mathbb{Q}[t]/(h(t))$.

Note that if s_2 is prime to p then the Jacobian is ordinary [Ho, p. 2366]. Also, if K can be written in the form $K = \mathbb{Q}(i\sqrt{a+b\sqrt{d}})$, with $a, b, d \in \mathbb{Z}$ and d and (a, b) square-free, then K is a primitive CM field (i.e. it contains no proper CM subfield) if and only if $a^2 - b^2d$ is not a square. We will assume K is a primitive quartic CM field throughout this paper.

2.2. Genus 2 curves and Igusa's j-invariants

In this section, we review Igusa's fundamental work on genus 2 curves and Siegel modular forms of genus 2. In his seminal work [Ig1], Igusa characterizes completely genus 2 curves over $\mathbb{Z}$ via 10 projective invariants, three quotients of which are the so-called (absolute) Igusa invariants j_1, j_2, j_3. They are enough to determine the curve over any field k of characteristic not equal to 2 if $j_1 \neq 0$. Assume that

$$X\colon\ y^2 = f(x)$$

is a (projective) genus 2 curve given by the above affine equation of degree 6. Let α_i be six roots of $f(x) = 0$, and write (ij) for $\alpha_i - \alpha_j$. Let u_0 be the leading coefficient of f. Then the three (absolute) Igusa invariants are defined as

$$j_1(X) = \frac{A^5}{D}, \qquad j_2(X) = \frac{A^3B}{D}, \qquad j_3(X) = \frac{A^2C}{D}, \tag{2.2}$$

where A, B, C, and D are integral Igusa invariants defined as (van Wamelen denoted them by I_2, I_4, I_6, and I_{10} respectively in [vW, p. 313])

$$\begin{aligned}
A &= u_0^2 \sum_{15} (12)^2(34)^2(56)^2,\\
B &= u_0^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2,\\
C &= u_0^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2,\\
D &= u_0^{10} \prod_{i<j} (ij)^2.
\end{aligned}$$

Here the subscript on the sums gives the number of possible combinations (of the same type) to sum over. In particular, when k is an algebraically closed field of characteristic not equal to 2, the function field of $\mathcal{C}_2$ over k is the rational function field $k(j_1, j_2, j_3)$ of three free variables. Here $\mathcal{C}_2$ is the moduli space of genus 2 curves, which is coarsely represented by an (open) quasi-projective subvariety of $\mathrm{Proj}(k[A, B, C, D])$ given by $D \neq 0$. Let $\mathcal{A}_2$ be the moduli space of principally polarized abelian surfaces. Then it is coarsely represented by the Siegel modular 3-fold $X_2 = \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2$. Igusa proved in [Ig2, Theorems 1 and 2] that the graded ring of holomorphic Siegel modular forms for $\mathrm{Sp}_2(\mathbb{Z})$ is the polynomial ring of ψ_4, ψ_6, χ_{10} and χ_{12}. Here

$$\psi_k(\tau) = \sum_{\gamma=\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\in P\backslash \mathrm{Sp}_2(\mathbb{Z})} \det(C\tau + D)^{-k} \tag{2.3}$$

is the normalized Eisenstein series of weight k for an even integer $k \geqslant 4$, where P is the standard Siegel parabolic subgroup of $\mathrm{Sp}_2(\mathbb{Z})$, and

$$\chi_{10} = -2^{-12}3^{-5}5^{-2}7^{-1}53^{-1} \cdot 43\,867(\psi_4\psi_6 - \psi_{10}), \tag{2.4}$$

$$\chi_{12} = 2^{-13}3^{-7}5^{-3}7^{-2}337^{-1} \cdot 131 \cdot 593\big(3^2 7^2 \psi_4^3 + 2 \cdot 5^3 \psi_6^2 - 691\psi_{12}\big) \tag{2.5}$$

are Siegel modular cusp forms of weight 10 and 12 respectively. So every rational function on X_2, i.e., a meromorphic Siegel modular form of weight 0, is a rational function of these functions.

Since $X \mapsto J(X)$ (the Jacobian of X) is an open immersion from $\mathcal{C}_2$ to $\mathcal{A}_2$, the rational functions on $\mathcal{C}_2(\mathbb{C})$ are the same as rational functions on X_2. So we can write the Igusa invariants j_i as rational functions of ψ_4, ψ_6, χ_{10}, and χ_{12} [Ig3, p. 848].

$$\begin{aligned} j_1(\tau) &= 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^5}, \\ j_2(\tau) &= 2^{-3} \cdot 3^3 \frac{\psi_4 \chi_{12}^3}{\chi_{10}^4}, \\ j_3(\tau) &= 2^{-5} \cdot 3\left(\frac{\psi_6 \chi_{12}^2}{\chi_{10}^3} + 2^2 \cdot 3 \frac{\psi_4 \chi_{12}^3}{\chi_{10}^4}\right). \end{aligned} \tag{2.6}$$

Here $j_i(\tau) = j_i(X)$ if there is genus 2 curve X over $\mathbb{C}$ such that its Jacobian $J(X)$ is isomorphic to the abelian surface $A(\tau) = \mathbb{C}^2/(\mathbb{Z}^2\tau + \mathbb{Z}^2)$ associated to τ. When there is no such genus 2 curve X, which happens exactly when $\chi_{10}(\tau) = 0$, $j_i(\tau)$ is not well defined.

2.3. Relation with theta constants and integral modular forms

We also give an expression for the invariants in terms of theta constants. For $m = (m_1, m_2) \in (\mathbb{Z}/2)^4$, the theta constant $\theta_m(\tau)$ is a holomorphic modular form of weight 1/2 (for the principal congruence subgroup of $\mathrm{Sp}_2(\mathbb{Z})$ of level 2):

$$\theta_m(\tau) = \sum_{n\in\mathbb{Z}^2} e\left(\frac{1}{2}(n + m_1/2)\tau(n + m_1/2)^t + (n + m_1/2)m_2^t\right). \tag{2.7}$$

θ_m is not identically zero if and only if m is even, i.e., $m_1 m_2^t = 0$ in $\mathbb{Z}/2$. There are 10 even theta constants. Then we have by [Ig3, p. 848]

$$\begin{aligned}
\psi_4 &= 2^{-2}\sum(\theta_m)^8,\\
\psi_6 &= \sum \pm(\theta_{m_1}\theta_{m_2}\theta_{m_3})^4,\\
-4\chi_{10} &= 2^{-12}\prod(\theta_m)^2,\\
12\chi_{12} &= 2^{-15}\sum(\theta_{m_1}\theta_{m_2}\theta_{m_3}\theta_{m_4}\theta_{m_5}\theta_{m_6})^4.
\end{aligned} \tag{2.8}$$

We refer to [Ig3, p. 848] for the determination of the sign in the second summation. In [Ig4], Igusa further proved the following fact, which is important arithmetically: ψ_4, ψ_6, $-4\chi_{10}$, $12\chi_{12}$ have integral Fourier coefficients which are relatively prime.

3. The map from a Hilbert modular surface to the Siegel modular 3-fold

In this section, we review a well-known symmetric map from a Hilbert modular surface to the Siegel modular 3-fold, make it explicit, and work out the Fourier expansion of the pullback of a holomorphic Siegel modular form under this map.

Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field with prime discriminant $D \equiv 1 \bmod 4$, and let $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$ be the non-trivial Galois conjugate of F over $\mathbb{Q}$. Let $\epsilon > 0$ be a unit such that $\sigma(\epsilon)\epsilon = -1$. Let $X = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$ be the open Hilbert modular surface.

Let $\mathrm{Sp}_2(\mathbb{Z})$ be the symplectic group over $\mathbb{Z}$ of genus two, consisting of 4×4-integral matrices g satisfying

$$gJg^t = J, \quad J = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$$

where I_2 is the identity matrix of order 2. Let

$$\mathbb{H}_2 = \left\{ \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in M_2(\mathbb{C})\colon \operatorname{Im}\tau > 0 \right\}$$

be the Siegel upper half-plane of genus two, and let

$$X_2 = \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2$$

be the open Siegel modular 3-fold. Here $\mathrm{Sp}_2(\mathbb{R})$ acts on $\mathbb{H}_2$ via

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\tau = (A\tau + B)(C\tau + D)^{-1}.$$

For $z = (z_1, z_2)$ and $a \in F$, we denote $z^* = \mathrm{diag}(z_1, z_2)$, and $a^* = \mathrm{diag}(a, \sigma(a))$. We also denote

$$\gamma^* = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}, \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F).$$

Choose a $\mathbb{Z}$-basis $\{e_1, e_2\}$ for $\mathcal{O}_F$:

$$\mathcal{O}_F = \mathbb{Z}e_1 + \mathbb{Z}e_2, \tag{3.1}$$

and define

$$R = \begin{pmatrix} e_1 & e_2 \\ \sigma(e_1) & \sigma(e_2) \end{pmatrix}. \tag{3.2}$$

We define the maps

$$\phi : \mathbb{H}^2 \to \mathbb{H}_2, \quad \phi(z) = R^t \operatorname{diag}\left(\frac{\epsilon}{\sqrt{D}} z_1, \sigma\left(\frac{\epsilon}{\sqrt{D}} \right) z_2 \right) R, \tag{3.3}$$

and

$$\begin{aligned} &\phi : \mathrm{SL}_2(F) \to \mathrm{Sp}_2(\mathbb{Q}), \quad \phi(\gamma) = S\gamma^* S^{-1}, \\ &S = \operatorname{diag}\left(R^t, R^{-1}\right) \operatorname{diag}\left(I_2, \left(\frac{\sqrt{D}}{\epsilon} \right)^* \right). \end{aligned} \tag{3.4}$$

It is easy to check that $\phi(\mathrm{SL}_2(\mathcal{O}_F)) \subset \mathrm{Sp}_2(\mathbb{Z})$. The next proposition asserts that the maps ϕ are compatible with the group actions.

Proposition 3.1. *The map ϕ defined above gives a holomorphic map from X into X_2. Moreover, it is independent of the choice of the $\mathbb{Z}$-basis $\{e_1, e_2\}$, and is symmetric in the sense that $\phi(z_1, z_2) = \phi(z_2, z_1)$ (as a map from X into X_2).*

Proof. This is a well-known result. We give a direct proof here for the convenience of the reader. Let

$$\mathrm{SL}_2(\mathcal{O}_F + \partial_F) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F) \colon\ a, d \in \mathcal{O}_F,\ b \in \partial_F^{-1},\ c \in \partial_F \right\},$$

where $\partial_F = \sqrt{D}\mathcal{O}_F$ is the different of F. Then it is easy to see that

$$\begin{aligned} \phi_0(z_1, z_2) &= \left(\frac{\epsilon}{\sqrt{D}} z_1, -\frac{\sigma(\epsilon)}{\sqrt{D}} z_2 \right), \\ \phi_0(\gamma) &= \operatorname{diag}\left(1, \frac{\sqrt{D}}{\epsilon} \right) \gamma \operatorname{diag}\left(1, \frac{\sqrt{D}}{\epsilon} \right)^{-1} \end{aligned}$$

gives an isomorphism between X and $X' = \mathrm{SL}_2(\mathcal{O}_F + \partial_F)\backslash\mathbb{H}^2$. So it suffices to verify that

$$\phi_1(z) = R^t z^* R, \qquad \phi_1(\gamma) = \operatorname{diag}\left(R^t, R^{-1}\right) \gamma^* \operatorname{diag}\left(R^t, R^{-1}\right)^{-1}$$

gives a holomorphic symmetric map from X' into X_2, which is independent of the choice of $\{e_1, e_2\}$. It is clearly holomorphic if well defined. We first check

$$\phi_1(\gamma z) = \phi_1(\gamma)\phi_1(z).$$

Indeed, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

$$\phi_1(\gamma) = \begin{pmatrix} R^t a^* R^{t,-1} & R^t b^* R \\ R^{-1} c^* R^{t,-1} & R^{-1} d^* R \end{pmatrix},$$

and so

$$\begin{aligned}\phi_1(\gamma)\phi_1(z) &= \big(R^t a^* z^* R + R^t b^* R\big)\big(R^{-1}c^* z^* R + R^{-1} d^* R\big)^{-1}\\ &= R^t\big(a^* z^* + b^*\big)\big(c^* z^* + d^*\big)^{-1} R\\ &= R^t(\gamma z)^* R\\ &= \phi_1(\gamma z),\end{aligned}$$

as claimed. So ϕ_1 is a well-defined map from X' to X_2. Next if $\{f_1, f_2\}$ is another $\mathbb{Z}$-basis of $\mathcal{O}_F$, write

$$(e_1, e_2) = (f_1, f_2)g, \quad g \in \mathrm{GL}_2(\mathbb{Z}).$$

Then

$$R(e_1, e_2) = R(f_1, f_2)g.$$

Here we use $R(e_1, e_2)$ for R to indicate its dependence on the basis. Similarly, one has

$$\phi_{1,e_1,e_2}(z) = g^t \phi_{1,f_1,f_2}(z) g = A(\phi_{1,f_1,f_2}) = \phi_{1,e_1,e_2}(z) \in X_2,$$

since $A = \mathrm{diag}(g^t, g^{-1}) \in \mathrm{Sp}_2(\mathbb{Z})$. Finally, to check that ϕ_1 is symmetric, notice that

$$\phi_1(z_2, z_1) = (wR)^t (z_1, z_2)^* (wR),$$

where $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and wR is the matrix associated to the $\mathbb{Z}$-basis $\{\sigma(e_1), \sigma(e_2)\}$ of $\mathcal{O}_F$. □

Proposition 3.2.

(1) *Let g be a holomorphic Hilbert modular form of $\mathrm{SL}_2(\mathcal{O}_F)$ of weight k. Then it has Fourier expansion*

$$g(z) = a_g(0) + \sum_{t = ae_1 + be_2 \in \mathcal{O}_F^+} a_g(t) q_1^a q_2^b.$$

Here the superscript $+$ stands for totally positive in this paper, and $q_j = e^{2\pi i(\frac{\epsilon e_j}{\sqrt{D}} z_1 + \sigma(\frac{\epsilon e_j}{\sqrt{D}}) z_2)}$.

(2) *Let*

$$f(\tau) = a_f(0) + \sum_{T \in \mathrm{Sym}_2(\mathbb{Z})^{\vee,+}} a_f(T) q^T$$

be a holomorphic Siegel modular form for $\mathrm{Sp}_2(\mathbb{Z})$ of weight k. Then its pullback $g = \phi^* f$ is a symmetric Hilbert modular form with the following Fourier expansion.

$$g(z) = f\big(\phi(z)\big) = a_g(0) + \sum_{t = ae_1 + be_2 \in \mathcal{O}_F^+} a_g(t) q_1^a q_2^b$$

with $a_g(0) = a_f(0)$ *and*

$$a_g(t) = \sum_{\substack{T \in \mathrm{Sym}_2(\mathbb{Z})^{\vee,+} \\ Q_T(e_1,e_2)=t}} a_f(T).$$

Here

$$Q_T(x_1, x_2) = (x_1, x_2) T \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

is the (*positive definite*) *quadratic form associated to* T, *and*

$$\mathrm{Sym}_2(\mathbb{Z})^{\vee} = \left\{ T = \begin{pmatrix} m_1 & \frac{1}{2}m \\ \frac{1}{2}m & m_2 \end{pmatrix} : m_i, m \in \mathbb{Z} \right\}$$

is the dual of $\mathrm{Sym}_2(\mathbb{Z})$. *Finally* $q^T = e^{2\pi i \operatorname{tr} T\tau}$.

Proof. (1) is the standard Fourier expansion with slight renormalization, writing $\nu \in \partial_F^{-1,+}$ as $\nu = \frac{\epsilon}{\sqrt{D}} t$ with $t = ae_1 + be_2 \in \mathcal{O}_F^+$.

(2) follows from the definition of ϕ and the simple fact

$$\operatorname{tr} T\phi(z) = \operatorname{tr} T R^t z^* R = Q_T(e_1, e_2) z_1 + \sigma\big(Q_T(e_1, e_2)\big) z_2. \qquad \square$$

Now we restrict ourselves to the example $F = \mathbb{Q}(\sqrt{5})$. Take

$$\epsilon = \frac{1+\sqrt{5}}{2}, \qquad \sigma(\epsilon) = \frac{1-\sqrt{5}}{2},$$

and $e_1 = 1$, $e_2 = \sigma(\epsilon)$. Then the equation $Q_T(e_1, e_2) = t = a + b\sigma(\epsilon) = a + b\frac{1-\sqrt{5}}{2}$ is equivalent to the following conditions

$$\begin{cases} m_1, m_2 \in \mathbb{Z}^+, \quad m \in \mathbb{Z}, \\ m^2 < 4m_1 m_2, \\ m_1 + m_2 = a, \\ m + m_2 = b. \end{cases} \tag{3.5}$$

We restate Proposition 3.2 as a corollary in this special case for use in the rest of the paper.

Corollary 3.3. *Assume* $F = \mathbb{Q}(\sqrt{5})$, *and let* $\epsilon = \frac{1+\sqrt{5}}{2}$. *Let*

$$\phi : \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2 \to \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2,$$

$$\phi(z) = \begin{pmatrix} 1 & 1 \\ \sigma(\epsilon) & \epsilon \end{pmatrix} \begin{pmatrix} \frac{\epsilon}{\sqrt{5}} z_1 & 0 \\ 0 & -\frac{\sigma(\epsilon)}{\sqrt{5}} z_2 \end{pmatrix} \begin{pmatrix} 1 & \sigma(\epsilon) \\ 1 & \epsilon \end{pmatrix} = \begin{pmatrix} \frac{\epsilon}{\sqrt{5}} z_1 - \frac{\sigma(\epsilon)}{\sqrt{5}} z_2 & \frac{z_2 - z_1}{\sqrt{5}} \\ \frac{z_2 - z_1}{\sqrt{5}} & -\frac{\sigma(\epsilon)}{\sqrt{5}} z_1 + \frac{\epsilon}{\sqrt{5}} z_2 \end{pmatrix}$$

be the map defined above, and let $e(z) := e^{2\pi iz}$ *and*

$$q_1 = e\left(\frac{\epsilon}{\sqrt{5}}z_1 - \frac{\sigma(\epsilon)}{\sqrt{5}}z_2\right) = e\left(\frac{1+\sqrt{5}}{2\sqrt{5}}z_1 - \frac{1-\sqrt{5}}{2\sqrt{5}}z_2\right), \qquad q_2 = e\left(\frac{z_2 - z_1}{\sqrt{5}}\right).$$

Then for a holomorphic Siegel modular form f *of weight* k *for* $\mathrm{Sp}_2(\mathbb{Z})$, $g = \phi^* f$ *is a symmetric holomorphic Hilbert modular form for* $\mathrm{SL}_2(\mathcal{O}_F)$ *with the Fourier expansion*:

$$g(z) = a_f(0) + \sum_{t=a+b\frac{1-\sqrt{5}}{2}\in\mathcal{O}_F^+} a_g(t)q_1^a q_2^b,$$

with

$$a_g(t) = \sum_{\text{condition (3.5)}} a_f\left(\begin{pmatrix} m_1 & \frac{1}{2}m \\ \frac{1}{2}m & m_2 \end{pmatrix}\right).$$

4. Hilbert modular forms and pullback of Igusa invariants

Let the notation be as in the end of Section 3. In particular $F = \mathbb{Q}(\sqrt{5})$ and $\epsilon = \frac{1+\sqrt{5}}{2}$. We first recall some basic facts on symmetric Hilbert modular forms for $\mathrm{SL}_2(\mathcal{O}_F)$, and refer to [Gu,Nag] for details. First recall the Eisenstein series of even weight $k \geqslant 2$:

$$G_k(z) = 1 + \sum_{t=a+b\frac{1-\sqrt{5}}{2}\in\mathcal{O}_F^+} b_k(t)q_1^a q_2^b, \tag{4.1}$$

where

$$b_k(t) = \kappa_k \sum_{(\mu)\supset(t)} \mathrm{N}(\mu)^{k-1}. \tag{4.2}$$

Here

$$\kappa_k = \frac{(2\pi)^{2k}\sqrt{5}}{(k-1)!^2 5^k \zeta_F(k)}$$

is a rational number, (μ) denotes the principal ideal $\mu\mathcal{O}_F$, and $\mathrm{N}(\mu) = \#\mathcal{O}_F/(\mu)$. Here are some values of κ_k:

$$\kappa_k = \begin{cases} 2^3\cdot 3\cdot 5 & \text{if } k=2, \\ 2^4\cdot 3\cdot 5 & \text{if } k=4, \\ \frac{1}{67}\cdot 2^3\cdot 3^2\cdot 5\cdot 7 & \text{if } k=6, \\ \frac{1}{412751}\cdot 2^3\cdot 3\cdot 5^2\cdot 11 & \text{if } k=10. \end{cases}$$

A simple calculation gives the first few coefficients for

$$0 < a \leqslant 3, \qquad \frac{1-\sqrt{5}}{2}a < b < \frac{1+\sqrt{5}}{2}a$$

as follows

$$\begin{aligned} G_k(z) = 1 &+ \kappa_k(1+q_2)q_1 + \kappa_k\big[q_2^{-1} + \big(1+4^{k-1}\big) + \big(1+5^{k-1}\big)q_2 + \big(1+4^{k-1}\big)q_2^2 + q_2^3\big]q_1^2 \\ &+ \kappa_k\big[\big(1+5^{k-1}\big)q_2^{-1} + \big(1+9^{k-1}\big) + \big(1+11^{k-1}\big)q_2 + \big(1+11^{k-1}\big)q_2^2 \\ &+ \big(1+9^{k-1}\big)q_2^3 + \big(1+5^{k-1}\big)q_2^4\big]q_1^3. \end{aligned} \tag{4.3}$$

A Hilbert modular form f is called symmetric if $f(z,z') = f(z',z)$ for $(z,z') \in \mathbb{H}^2$. Notice that the Eisenstein series G_k are all symmetric. We call it integral if all its Fourier coefficients are integral, and call it primitively integral if furthermore its Fourier coefficients have greatest common divisor 1. For a ring R, we denote

$$M^{\mathrm{Sym}}\big(\mathrm{SL}_2(\mathcal{O}_F), R\big) = \sum_{k\geqslant 0} M_k^{\mathrm{Sym}}\big(\mathrm{SL}_2(\mathcal{O}_F), R\big)$$

for the graded ring of holomorphic symmetric Hilbert modular forms of $\mathrm{SL}_2(\mathcal{O}_F)$ with Fourier coefficients in R. When $R = \mathbb{Z}$, we drop R in the notation. We will need the following theorems in this paper.

Theorem 4.1. *(See [Nag, Theorem 2].) Let*

$$\begin{aligned} \theta_6 &= -\frac{67}{2^5 3^3 5^2}\big(G_6 - G_2^3\big), \\ \theta_{10} &= 2^{-10}3^{-5}5^{-5}7^{-1}\big(412751G_{10} - 5\cdot 67\cdot 2293G_2^2G_6 + 2^2\cdot 3\cdot 7\cdot 4231G_2^5\big), \\ \theta_{12} &= 2^{-2}\big(\theta_6^2 - G_2\theta_{10}\big). \end{aligned} \tag{4.4}$$

Then the functions G_2, θ_6, θ_{10}, and θ_{12} are primitively integral symmetric Hilbert modular forms, and are a minimal set of generators for $M^{\mathrm{Sym}}(\mathrm{SL}_2(\mathcal{O}_F), \mathbb{Z})$.

In [Nag], θ_i are denoted by J_i.

Theorem 4.2 *(Gundlach).*

(1) *The ring of symmetric holomorphic Hilbert modular forms for $\mathrm{SL}_2(\mathcal{O}_F)$ is a polynomial ring of G_2, G_6, and θ_{10}. In particular,*

$$\dim M_k^{\mathrm{Sym}}\big(\mathrm{SL}_2(\mathcal{O}_F)\big) = \#\big\{(x,y,z) \in \mathbb{Z}^3_{\geqslant 0}\colon\ x+3y+5z = k/2\big\}.$$

(2) *The field of symmetric meromorphic Hilbert modular functions for $\mathrm{SL}_2(\mathcal{O}_F)$ are rational functions of*

$$J_1 = \frac{\theta_6}{G_2^3} \quad \text{and} \quad J_2 = \frac{G_2^5}{\theta_{10}}.$$

Proof. Claim (1) is exactly [Gu, Satz 5]. Claim (2) clearly follows from [Gu, Satz 6] since

$$\theta_6 = -\frac{67}{2^5 3^3 5^2}\big(G_6 - G_2^3\big). \qquad \square$$

We call J_1 and J_2 the *Gundlach invariants* in this paper.

Remark 4.3. Alternative choices for the two invariants present different trade-offs for efficient computation. For example, one could use the invariants J_1 and J_3, where

$$J_3 = J_1 + J_2^{-1} = \frac{\theta_6 G_2^2 + \theta_{10}}{G_2^5}.$$

This choice has the advantage that both invariants are rather small. Another possible choice would be to use invariants J_2 and J_4 where

$$J_4 = J_1 J_2 = \frac{\theta_6 G_2^2}{\theta_{10}}.$$

This choice has the advantage that both invariants have denominator θ_{10}.

4.1. Pullback of Igusa invariants

It turns out that θ_i are pullbacks of Siegel modular forms. Indeed, Resnikoff proved in [Re, Theorem 1] the following theorem.

Theorem 4.4.

$$\begin{aligned}
\phi^*\psi_4 &= G_2^2,\\
\phi^*\psi_6 &= -\frac{42}{25}G_2^3 + \frac{67}{25}G_6 = G_2^3 - 2^5 3^3 \theta_6,\\
-4\phi^*\chi_{10} &= \theta_{10},\\
12\phi^*\chi_{12} &= 3\theta_6^2 - 2G_2\theta_{10}.
\end{aligned} \tag{4.5}$$

In particular, θ_{10} is 2^{-12} times the square of the product of the ten Hilbert theta constants defined in [Gu, Section 2], i.e.,

$$\theta_{10} = 2^{-12}\Theta^2 \tag{4.6}$$

where Θ is the weight 5 modular form defined by Gundlach. This identity (or more precisely the identity in Theorem 4.1 describing Θ^2) is given [Nag, Lemma 5.1] and is implicitly proved in [Gu]. We will use this fact in Section 5. A short calculation leads to the following proposition expressing the pullback of Igusa's functions in terms of the Gundlach invariants.

Proposition 4.5. *One has*

$$\begin{aligned}
\phi^* j_1 &= 8J_2\left(3J_1^2J_2 - 2\right)^5,\\
\phi^* j_2 &= \frac{1}{2}J_2\left(3J_1^2J_2 - 2\right)^3,\\
\phi^* j_3 &= 2^{-3}J_2\left(3J_1^2J_2 - 2\right)^2\left(4J_1^2J_2 + 2^5\cdot 3^2 J_1 - 3\right).
\end{aligned}$$

5. CM points and CM values of J_1 and J_2

In this section we explain how to generate CM points on the Hilbert moduli space and give an algorithm for computing genus 2 curves from Gundlach invariants.

Let $K = F(\sqrt{\Delta})$ be a non-biquadratic quartic CM extension of $F = \mathbb{Q}(\sqrt{5})$. We briefly review the construction of CM points and refer to [BY, Section 3] and references there for details. Let $\Phi = \{\sigma_1, \sigma_2\}$ be a CM type of K. A CM point in $X = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$ of CM type $(\mathcal{O}_K, \Phi)$ is the image of a point $\Phi(z) = (\sigma_1(z), \sigma_2(z)) \in \mathbb{H}^2$, where $z \in K$ satisfies the condition that $\Lambda_z = \mathcal{O}_F + \mathcal{O}_F z$ is a fractional ideal. Conversely, if $\mathfrak{a}$ is a fractional ideal of K, one can write

$$\mathfrak{a} = \mathcal{O}_F\alpha + \mathcal{O}_F\beta, \quad \alpha, \beta \in \mathfrak{a}$$

since F has class number one. Furthermore since F has a unit of norm -1, one can find generators α and β (multiplying by such a unit if necessary) such that $\Phi(\frac{\beta}{\alpha}) \in \mathbb{H}^2$. So $z = \frac{\beta}{\alpha}$ gives a CM point $\Phi(z)$ of CM type $(\mathcal{O}_K, \Phi)$, and its associated lattice is $\Lambda_z = \alpha^{-1}\mathfrak{a}$. Moreover, this CM point $z \in X$ depends only on the ideal class $[\mathfrak{a}]$ of $\mathfrak{a}$, and we denote it by $z(\mathfrak{a}, \Phi)$ or $z([\mathfrak{a}], \Phi)$. One can prove that the correspondence $[\mathfrak{a}] \mapsto z([\mathfrak{a}], \Phi)$ gives rise to a bijection between the ideal class group $\mathcal{CL}(K)$ and the set of CM points of CM type $(\mathcal{O}_K, \Phi)$. The inverse is $z \mapsto [\Lambda_z]$.

Write $\mathrm{CM}(K, \Phi)$ as the formal sum of the CM points of CM type $(\mathcal{O}_K, \Phi)$, and view it as a 0-cycle in X. Recall that X has a canonical model over $\mathbb{Q}$ (as the coarse moduli space of ∂_F^{-1}-polarized abelian surfaces with real multiplication by $\mathcal{O}_F$) (see for example [Ge]). Then $\mathrm{CM}(K, \Phi)$ is actually defined over the reflex field $\tilde{K}$ of (K, Φ) (as moduli space of ∂_F^{-1}-polarized abelian surfaces with complex multiplication by $\mathcal{O}_K$ with an extra condition on differentials related to Φ). Moreover, let $\Phi' = \{\sigma_1, \bar{\sigma}_2\}$ be another CM type, then $\mathrm{CM}(K) = \mathrm{CM}(K, \Phi) + \mathrm{CM}(K, \Phi')$ is defined over $\mathbb{Q}$ [BY, Lemma 3.4]. Furthermore, the same lemma asserts that $\mathrm{CM}(K, \Phi)$ is defined over $\mathbb{Q}$ itself when K is cyclic. Notice also that if $\Phi(z)$ is a CM point of CM type $(\mathcal{O}_K, \Phi)$ associated to the ideal $\mathfrak{a}$, then $\Phi'(\epsilon z) = (\sigma_1(\epsilon z), \overline{\sigma_2(\epsilon z)})$ is a CM point of CM type $(\mathcal{O}_K, \Phi')$ associated to the same ideal $\mathfrak{a}$, where ϵ is a unit of F such that $\sigma_1(\epsilon) > 0$ and $\sigma_2(\epsilon) < 0$.

Now let $J = J_1$ or J_2. Then J is a rational function on X, $J(z)$ is algebraic over $\mathbb{Q}$, and

$$J\big(\mathrm{CM}(K)\big) = \prod_{z \in \mathrm{CM}(K)} J(z) \in \mathbb{Q}.$$

However, $J(z)$ is not an algebraic integer and $J(\mathrm{CM}(K))$ is not an integer. To compute $J(z)$ practically (which is the purpose of this paper), we need an upper bound for the denominators of the coefficients of the minimal polynomial. This can be done by the main results in [BY,Ya2]. We first need some notation. Let $\tilde{K}$ be the reflex field of (K, Φ). It is also a quartic CM number field with real quadratic subfield $\tilde{F}$. Let $d_{K/F}$ be the relative discriminant of K/F and d_K be the absolute discriminant of K. For a nonzero element $t \in d_{\tilde{K}/\tilde{F}}^{-1}$ and a prime ideal $\mathfrak{l}$ of $\tilde{F}$, we define

$$B_t(\mathfrak{l}) = \begin{cases} 0 & \text{if } \mathfrak{l} \text{ is split in } \tilde{K}, \\ (\mathrm{ord}_{\mathfrak{l}}\, t + 1)\rho(t d_{\tilde{K}/\tilde{F}} \mathfrak{l}^{-1}) \log|\mathfrak{l}| & \text{if } \mathfrak{l} \text{ is non-split in } \tilde{K}, \end{cases} \tag{5.1}$$

and

$$B_t = \sum_{\mathfrak{l}} B_t(\mathfrak{l}). \tag{5.2}$$

Here $|\mathfrak{l}|$ is the norm of $\mathfrak{l}$, and $\rho(\mathfrak{a}) = \rho_{\tilde{K}/\tilde{F}}(\mathfrak{a})$ is defined as

$$\rho(\mathfrak{a}) = \#\{\mathfrak{A} \subset \mathcal{O}_{\tilde{K}} \colon N_{\tilde{K}/\tilde{F}}\mathfrak{A} = \mathfrak{a}\}. \tag{5.3}$$

For a positive integer $m > 0$, set

$$b_m = \sum_{\substack{t=\frac{n+m\sqrt{q}}{2p} \in d_{\tilde{K}/\tilde{F}}^{-1} \\ |n|<m\sqrt{q}}} B_t. \tag{5.4}$$

Notice that e^{b_m} are positive integers. Finally, let W_K be the number of roots of unity in K, one has

$$W_K = \begin{cases} 10 & \text{if } K = \mathbb{Q}(e(1/5)), \\ 2 & \text{otherwise.} \end{cases}$$

Proposition 5.1. *Let the notation be as above, and let $h = h_K$ be the ideal class number of K. Assume that $G_2(z) \neq 0$, and $d_K = 5^2 q$ for a prime $q \equiv 1 \bmod 4$.*

(1) *Let*

$$P_2(x) = \prod_{z \in \mathrm{CM}(K)} \big(x - J_2(z)\big) = \sum_{i=0}^{2h} a_i(J_2) x^i \in \mathbb{Q}[x].$$

Then $a_i(J_2) \in \mathbb{Q}$ with denominator being a factor of $e^{\frac{W_K}{2} b_1}$. Moreover, $a_0(J_2) = (\frac{n^5}{e^{b_1}})^{\frac{W_K}{2}}$ for some integer n.

(2) *Let*

$$P_1(x) = \prod_{z \in \mathrm{CM}(K)} \big(x - J_1(z)\big) = \sum_{i=0}^{2h} a_i(J_1) x^i \in \mathbb{Q}[x].$$

Then $a_i(J_1) \in \mathbb{Q}$ with denominator being a factor of $n^{\frac{3W_K}{2}}$.

Proof. The proof is very similar to that of [Ya2, Theorem 1.7]. We sketch it here for the convenience of the reader. We use the notation in [Ya2], and refer to [Ya2] for explanation of the Arakelov intersection theory used here. Let $\mathcal{X}$ be the moduli stack over $\mathbb{Z}$ of ∂_F^{-1}-polarized abelian surfaces with real multiplication by $\mathcal{O}_F$, and let $\mathcal{CM}(K)$ be the moduli stack over $\mathbb{Z}$ of ∂_F^{-1}-polarized abelian surfaces with real multiplication by $\mathcal{O}_K$. Then $\mathcal{CM}(K)(\mathbb{C}) = 2\,\mathrm{CM}(K)$ by [Ya2, Lemma 3.2]. By [BY, Section 10], $\operatorname{div}\theta_{10} = \mathcal{T}_1$, where $\mathcal{T}_1$ is the first arithmetic Hirzebruch–Zagier divisor in $\mathcal{X}$ (moduli space of $E \otimes \mathcal{O}_F$, where E are elliptic curves). The modular form θ_{10} is denoted by Ψ_5^2 in [BY]. So the Arakelov intersection theory gives

$$\begin{aligned} 0 &= h_{\widehat{\operatorname{div}(J_2)}}\big(\mathcal{CM}(K)\big) \\ &= 5\mathcal{CM}(K).\operatorname{div} G_2 - 2\mathcal{CM}(K).\mathcal{T}_1 - \frac{1}{W_K}\log\big|\mathcal{CM}(K)(\mathbb{C})\big| \\ &= 5\mathcal{CM}(K).\operatorname{div} G_2 - 2\mathcal{CM}(K).\mathcal{T}_1 - \frac{2}{W_K}\log\big|J_2\big(\mathrm{CM}(K)\big)\big|. \end{aligned}$$

So

$$\frac{2}{W_K}\log\big|J_2\big(\mathrm{CM}(K)\big)\big| = 5\mathcal{CM}(K).\operatorname{div} G_2 - 2\mathcal{CM}(K).\mathcal{T}_1.$$

By [Ya1, Theorem 1.2] or [Ya2, Theorem 1.2], one has

$$\mathcal{CM}(K).\mathcal{T}_1 = \frac{1}{2}b_1.$$

So

$$\left|a_0(J_2)\right| = \left|J_2\big(\mathrm{CM}(K)\big)\right| = \left(\frac{|n|^5}{e^{b_1}}\right)^{\frac{W_K}{2}}$$

as claimed, where $n \in \mathbb{Z}$ with

$$\log|n| = \mathcal{CM}(K).\operatorname{div} G_2.$$

For a general i. Let L be the field generated by all $J_2(z)$, $z \in \mathrm{CM}(K)$. One can then write by unique factorization of ideals of $\mathcal{O}_L$,

$$J_2(z_i) = \mathfrak{a}_i\mathfrak{b}_i^{-1} \in \mathfrak{b}_i^{-1}$$

for $z_1, \ldots, z_{2h} \in \mathrm{CM}(K)$, where $\mathfrak{a}_i$ and $\mathfrak{b}_i$ are relatively prime integral ideals of L. Then

$$a_0\mathcal{O}_L = \prod J_2(z_i)\mathcal{O}_L = \Big(\prod \mathfrak{a}_i\Big)\Big(\prod \mathfrak{b}_i\Big)^{-1} = \frac{n^{\frac{5W_K}{2}}}{e^{\frac{W_K}{2}b_1}}.$$

If we write $a_0 = \frac{A}{B}$ with $A, B \in \mathbb{Z}$ relatively prime, then

$$\prod \mathfrak{a}_i = A\mathcal{O}_L, \qquad \prod \mathfrak{b}_i = B$$

and $B | e^{\frac{W_K}{2}b_1}$ (n and e^{b_1} might not be relatively prime). Now

$$a_i = (-1)^i \sum_{j_1,\ldots,j_i} \prod_{k=1}^{i} J_2(z_{j_k}) \in \Big(\prod \mathfrak{b}_i\Big)^{-1} = B^{-1}\mathcal{O}_L,$$

and so a_i has denominator dividing B, and thus dividing $e^{\frac{W_K}{2}b_1}$. This proves (1). One can prove (2) the same way using the just proved fact:

$$\mathcal{CM}(K).\operatorname{div} G_2 = \log|n|$$

(replacing $\mathcal{CM}(K).\operatorname{div}\theta_{10} = 2\mathcal{CM}(K).\mathcal{T}_1 = b_1$). □

5.1. Algorithm for computing Gundlach invariants and CM curves

To actually compute $J_i(z)$ for a CM point, we give the following explicit algorithm.

Algorithm 5.1.
Input: K a primitive quartic CM field, p a prime which splits completely into principal ideals in K^*, the reflex of K, and S a collection of 2 or 4 possible group orders for Jacobians of genus 2 curves over $\mathbb{F}_p$ with CM by K.

Output: Gundlach invariants modulo p for genus 2 curves with CM by K and equations for curves C over $\mathbb{F}_p$ with $\#J(C) \in S$.

1. Find $\Delta \in \mathcal{O}_F$ such that Δ is totally negative and $\Delta\sigma(\Delta) = q \equiv 1 \pmod 4$ is a prime (not essential). In such a case, $K = F(\sqrt{\Delta})$ is a non-Galois quartic CM field if $q \neq 5$. Moreover, one can find

$$\mathcal{O}_K = \mathcal{O}_F + \mathcal{O}_F \frac{b_0 + \sqrt{\Delta}}{2}.$$

2. Let $M = \mathbb{Q}(\sqrt{\Delta}, \sqrt{\sigma(\Delta)})$ be the Galois closure of K over $\mathbb{Q}$. We fix one embedding of M into $\mathbb{C}$ and view then M as a subfield of $\mathbb{C}$ so that

$$\operatorname{Im}(\sqrt{\Delta}) > 0, \qquad \operatorname{Im}\bigl(\sqrt{\sigma(\Delta)}\bigr) > 0.$$

Let

$$\sigma(\sqrt{\Delta}) = \sqrt{\sigma(\Delta)}, \qquad \sigma\bigl(\sqrt{\sigma(\Delta)}\bigr) = -\sqrt{\Delta},$$

and

$$\tau(\sqrt{\Delta}) = \sqrt{\sigma(\Delta)}, \qquad \tau\bigl(\sqrt{\sigma(\Delta)}\bigr) = \sqrt{\Delta}.$$

Notice that $\sigma^2 = {}^-$ is complex conjugation on M, and $\sigma|_F$ is the non-trivial Galois element σ of $F/\mathbb{Q}$. Then $\operatorname{Gal}(M/\mathbb{Q}) \cong D_8$ is generated by σ and τ. K has four CM types

$$\Phi = \{1, \sigma\}, \qquad \Phi' = \bigl\{1, \sigma' = \sigma^3\bigr\}, \qquad \bar{\Phi} = \bigl\{{}^-, \bar{\sigma} = \sigma'\bigr\}, \quad \text{and} \quad \bar{\Phi}'.$$

One has

$$\operatorname{CM}(K) = \operatorname{CM}(K, \Phi) + \operatorname{CM}\bigl(K, \Phi'\bigr) = \operatorname{CM}(K, \bar{\Phi}) + \operatorname{CM}\bigl(K, \bar{\Phi}'\bigr).$$

3. Find the class number h_K and the ideals generating the class group of K.
4. Given an ideal $\mathfrak{a}$ of K, write

$$\mathfrak{a} = \left[a, \frac{b + \sqrt{\Delta}}{2}\right] = \mathcal{O}_F a + \mathcal{O}_F \frac{b + \sqrt{\Delta}}{2}$$

such that a is totally positive with $a\mathcal{O}_F = \mathrm{N}_{K/F}\,\mathfrak{a}$, and that $z = \frac{b+\sqrt{\Delta}}{2a}$.

$$z\bigl([\mathfrak{a}], \Phi\bigr) = \Phi(z) = (z, \sigma z) \in \mathbb{H}^2$$

is the CM point in $X = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$ associated to the ideal class $[\mathfrak{a}]$ and Φ. Moreover, one has in this case

$$z\big([\mathfrak{a}], \Phi'\big) = \Phi'\big(\epsilon z, \sigma'(\epsilon z)\big) \in \mathbb{H}^2$$

is the CM point of CM type Φ' associated to $\mathfrak{a}$.

5. Compute $J_i(z([\mathfrak{a}], \Phi))$ and $J_i(z([\mathfrak{a}], \Phi'))$, using the precision requirements from Proposition 5.1. Form the minimal polynomials $P_1(X)$ and $P_2(X)$. Reduce modulo a prime p not dividing the denominators and find roots (mod p).

6. Compute $\phi^* j_i$ (mod p) using the formulas in Proposition 4.5. Apply Mestre's algorithm (see Appendix A.2) to pairs of roots from step 5 to construct a genus 2 curve over the finite field $\mathbb{F}_p$.

6. Examples

We give two examples here to demonstrate Algorithm 5.1.

6.1. Example 1

Let $F = \mathbb{Q}(\sqrt{5})$ and K be the Galois cyclic CM field $\mathbb{Q}(\sqrt{-5+\sqrt{5}})$ of class number 2 defined by the polynomial $f(t) = t^4 + 10t^2 + 20$. Let x be a root of f. Then the ring of integers of K can be written as $\mathcal{O}_F + x\mathcal{O}_F$, representing the trivial ideal class. The other ideal class in $\mathcal{O}_K$ is represented by the ideal $2\mathcal{O}_F + x\mathcal{O}_F$. Since K is Galois cyclic, there is only one CM type up to isomorphism, and so we get only one polarized abelian surface for each ideal class.

Next we convert each ideal class into the corresponding CM point on the Hilbert moduli space, by letting $z = x$ and $z' = x/2$ and mapping $z \mapsto (\sigma_1(z), \sigma_2(z))$, such that $\mathrm{Im}(\sigma_i(z)) > 0$, for $i = 1, 2$. We evaluate $G(k)$ at $(\sigma_1(z), \sigma_2(z))$ for $k = 2, 4, 6, 10$ and compute θ_6 and θ_{10}. In this example the class equation fails to be irreducible, and both invariants of both ideal classes are rational (as opposed to satisfying a polynomial with rational coefficients).

Then the computed invariants are $J_1(z) = 1/194\,400 = 2^{-5}3^{-5}5^{-2}$ and $J_2(z) = 2^8 3^{10} 5^5$ and $J_1(z') = 1/864 = 2^{-5}3^{-3}$ and $J_2(z') = 194\,400\,000/121 = 2^8 3^5 5^5 11^{-2}$.

Using the formulas we found in Proposition 4.5, we compute the 3 Igusa invariants in terms of J_1 and J_2, and we find that they indeed match the Igusa invariants as calculated by van Wamelen in [vW]. For example, $\phi^* j_1(z') = 2 \cdot 3^{10} 5^5 719^5 / 11^{12}$.

Mestre's algorithm to generate a curve from its invariants is explained in Appendix A below, and has been implemented in Magma for example, and we use the Magma command `HyperellipticCurveFromIgusaClebsch` to generate the curve from the 4 Igusa Clebsch invariants: $I_2 = 1$, $I_{10} = I_2^5/j_1$, $I_4 = j_2 \cdot I_{10}/I_2^3$, and $I_6 = j_3 \cdot I_{10}/I_2^2$.

Current minimum security levels for genus 2 hyperelliptic curve cryptography require working over a field which is at least 128 bits, so that the group order is at least 256 bits. We find a prime of cryptographic size which splits completely into principal ideals in K, $p = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,213\,431$. One of the possible group orders for the Jacobian of a genus 2 curve over $\mathbb{F}_p$ with CM by K is

$$N = 115\,792\,089\,237\,316\,195\,439\,222\,313\,149\,717\,904\,948\,817\,631\,071\,168\,155\,151\,994\,257\,158\,091\,641\,307\,220.$$

We find a curve C whose Jacobian has order N with Gundlach invariants $J_1 = 1/194\,400$ and $J_2 = 47\,239\,200\,000$ defined over $\mathbb{F}_p$ by the equation:

$$\begin{aligned} C: y^2 = {} & 338\,931\,466\,186\,923\,884\,354\,352\,055\,023\,395\,682\,589 x^6 \\ & + 147\,253\,980\,567\,190\,107\,524\,376\,275\,221\,857\,804\,426 x^5 \\ & + 269\,300\,356\,029\,475\,808\,457\,260\,262\,457\,030\,252\,867 x^4 \end{aligned}$$

$$+ 138\,384\,226\,796\,715\,975\,861\,495\,440\,871\,003\,340\,679x^3$$
$$+ 49\,380\,499\,612\,684\,083\,483\,659\,413\,593\,343\,091\,406x^2$$
$$+ 49\,858\,147\,947\,087\,501\,179\,789\,824\,403\,795\,308\,130x$$
$$+ 228\,614\,259\,049\,869\,931\,400\,731\,578\,430\,276\,414\,286.$$

6.2. Example 2

Let $K = \mathbb{Q}[x]/(x^4 + 30x^2 + 180)$ be a Galois cyclic quartic CM field with class number 4.

A list of relative generators for the four ideal classes is $[z_1, z_2, z_3, z_4] = [1/x, 3/x, 2/x, 6/x]$. We will compute the minimal polynomials of the Gundlach invariants of the CM genus 2 curves, $P_1 = \prod_{i=1,h}(X - J_1(z_i))$ and $P_2 = \prod_{i=1,h}(X - J_2(z_i))$.

Calculating with 100 digits of precision, and computing the Hilbert Eisenstein series up to a bound of 60, we recognize the minimal polynomial of J_1 as

$$\begin{aligned}(\text{denominator}) \cdot P_1(X) = {} & 807\,620\,490\,521\,688\,228\,341\,760\,000\,000\,000X^4 \\ & - 673\,073\,974\,659\,036\,488\,878\,080\,000\,000X^3 \\ & + 65\,851\,509\,360\,835\,482\,658\,560\,000X^2 \\ & - 1\,301\,278\,988\,080\,300\,060\,800X + 826\,918\,614\,601,\end{aligned}$$

where the denominator is written as the coefficient of the degree 4 term. This was possible to recognize because the trace term (coefficient of X^3) was accurate enough to recognize as a rational number, and then multiplying through by this denominator was enough to make all the other coefficients recognizable as integers. The larger the imaginary part of a CM point, the faster the Hilbert Eisenstein series converge. In this case it was enough to compute two of the invariants up to a bound of 20.

Unfortunately, the same amount of accuracy does not suffice to recognize the minimal polynomial for J_2 because the size of $J_2(z_i)$ is much larger than $J_1(z_i)$, and the precision loss in multiplication is proportional to the size. This observation begs the interesting question of whether the invariants J_1, J_2 are the best choice for computation, and whether one of the alternatives given in Remark 4.3 might be better. Indeed θ_{10} is very small at CM points, which makes J_2 very large. However there is an advantage to working with an invariant which has θ_{10} as the denominator, since the geometric interpretation of the divisor of θ_{10} on the arithmetic moduli space leads to a formula for the factorization of the denominator. For example, with 100 digits of precision and a bound of 80 for the Hilbert Eisenstein series, the trace term can be recognized as $-(2^8 \cdot 3^4 \cdot 5^5 \cdot 43 \cdot 3943 \cdot 187\,784\,496\,127\,072\,321)/(11^2 \cdot 19^2 \cdot 31^2 \cdot 139^2)$ because the Bruinier–Yang formula explained in Proposition 5.1 predicts a multiple of the denominator, and multiplying through makes the coefficients into integers if they have been computed to sufficient accuracy.

However in this case, multiplying through by this denominator does not suffice to recognize the entire polynomial because the other coefficients were not computed with sufficient accuracy (roughly 54 digits of accuracy are missing). Recomputing one of the invariants with 200 digits of accuracy and a bound of 100 for the Hilbert Eisenstein series, and using some tricks to bootstrap from the coefficients which were already recognized exactly, we find the minimal polynomial:

$$\begin{aligned}(\text{denominator}) \cdot P_2(X) = {} & 94\,309\,255\,921\,730\,641X^4 \\ & - 239\,904\,685\,257\,879\,199\,493\,648\,103\,415\,200\,000X^3 \\ & + 513\,653\,659\,271\,447\,214\,497\,005\,427\,725\,467\,360\,000\,000\,000X^2 \\ & - 104\,766\,327\,156\,563\,190\,587\,332\,424\,648\,038\,320\,000\,000\,000\,000\,000\,000X \\ & + 392\,145\,514\,761\,205\,878\,288\,552\,914\,309\,761\,680\,000\,000\,000\,000\,000\,000\,000\,000.\end{aligned}$$

Taking a rational 128-bit prime which splits completely into principal ideals in K^*,

$$p = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,219\,931,$$

we find a possible 256-bit group order which is almost prime:

$$\begin{aligned} N &= 115\,792\,089\,237\,316\,195\,404\,406\,655\,439\,534\,933\,218\,761\,722\,676\,637\,023\,113\,527\,648\,931\,946\,009\,038\,580 \\ &= 2^2 \cdot 5 \cdot 5\,789\,604\,461\,865\,809\,770\,220\,332\,771\,976\,746\,660\,938\,086\,133\,831\,851\,155\,676\,382\,446\,597\,300\,451\,929. \end{aligned}$$

Applying Mestre's algorithm to the Gundlach invariants modulo p:

$$J_1 = 279\,214\,503\,502\,700\,065\,510\,996\,498\,564\,179\,588\,291$$

and

$$J_2 = 288\,623\,429\,461\,296\,121\,011\,774\,846\,415\,179\,312\,191,$$

we obtain the hyperelliptic curve defined over $\mathbb{F}_p$ by

$$\begin{aligned} y^2 = {} & 290\,539\,680\,218\,172\,865\,744\,314\,331\,157\,056\,329\,993x^6 \\ & + 17\,725\,362\,475\,694\,001\,839\,684\,832\,044\,029\,281\,717x^5 \\ & + 309\,288\,833\,050\,300\,807\,168\,917\,976\,953\,010\,217\,423x^4 \\ & + 228\,634\,886\,915\,584\,929\,858\,087\,477\,302\,355\,957\,630x^3 \\ & + 133\,246\,848\,479\,040\,973\,236\,010\,420\,879\,045\,116\,884x^2 \\ & + 226\,238\,451\,489\,753\,874\,682\,526\,142\,621\,565\,485\,775x \\ & + 51\,254\,902\,283\,888\,571\,906\,628\,040\,318\,549\,913\,376. \end{aligned}$$

7. Conclusion

It can already be seen in the examples given in Section 6 that the real difficulty in computing CM curves lies in the vast amount of high-precision computation which is done to evaluate these modular forms to high accuracy. By using Hilbert invariants we only have to compute two such values for each CM point, instead of three. While terms in the Fourier expansion for the Igusa functions are products of three exponential functions (of three variables), terms in the Fourier expansions for the Hilbert modular functions we define are products of *two* exponential functions (of *two* variables). This simplification results in fewer evaluations of exponential functions and fewer high-precision multiplications of values of exponential functions. Furthermore, the expression for and the calculation of the CM points on the Hilbert moduli space is significantly simpler than the calculation of the period matrices on the Siegel moduli space.

Once the rational coefficients of the class polynomials for K have been computed and recognized, finding the roots modulo p and using the formulas in Proposition 4.5 modulo p to recover the Igusa invariants modulo p is negligible from a computational perspective. A curve over the finite field with CM by K can then be generated by applying Mestre's algorithm to the Igusa invariants. Still it would be interesting to find an algorithm like Mestre's algorithm which reconstructs the curve directly from the invariants on the Hilbert moduli space without passing through the Igusa invariants.

Future work includes computing larger examples with the goal of adding more examples of class polynomials to Kohel's database [Ko]. The other algorithms for computing Igusa class polynomials via the Chinese Remainder Theorem [EL] and via p-adic arithmetic [GH] may also benefit from combining

ideas with this paper. Each method works well for a certain class of fields K, and our method works for K such that the real quadratic subfield is of a restricted form. We are also in the process of formalizing the complexity estimates for our algorithm, which will allow a more detailed comparison with the existing methods.

The main goals of this paper were to introduce and describe a new technique in a growing field of research and to note its apparent advantages over the standard complex analytic method on the Siegel moduli space. The authors hope that this result will encourage others to explore the relative advantages and benefits of computing Hilbert invariants compared to other methods (complex analytic, CRT, p-adic), determine where it might be best applicable, and whether it might be profitably combined with other techniques. These questions as well as that of extending this technique to higher genera and smaller modular functions are interesting and open lines of research.

Acknowledgments

This joint work was mainly done while the second author visited the Cryptography Group at Microsoft Research in Redmond in 2009, and he thanks Microsoft Research for providing an excellent working environment. Both authors thank the anonymous referees and Michael Naehrig for detailed comments to improve the paper.

Appendix A

A.1. Pari-gp code to compute Gundlach invariants

```
**************Computing the CM field and CM points***********
default(realprecision,50)
d=5
a=5
b=-1
k = bnfinit(y^2-d)
R = rnfinit(k,x^2-((-a-b*Mod(y,y^2-d))))
K = bnfinit(R[11][1])
h = bnfclgp(K)[1]
%% This computes generators for the ideal classes in the Galois cyclic case:
ilist = vector(h,i,0)
x1 = R[7][1][1]
x2 = R[7][1][2]
I1 = bnfisprincipal(k,R[7][2][1])[2]
g1 = I1[1]*k[7][7][1]+I1[2]*Mod(k[7][7][2],y^2-d)
I2 = bnfisprincipal(k,R[7][2][2])[2]
g2 = I2[1]*k[7][7][1]+I2[2]*Mod(k[7][7][2],y^2-d)
ilist[1] = (x1*g1)/(x2*g2)
%% This works for Galois cyclic fields with cyclic class group:
C1 = bnfclgp(K)[3][1];  C=1;
{for(i=1,h-1,
    C = idealmul(K,C,C1);
    RC = rnfidealabstorel(R,K.zk*C);
    z1 = (RC[1][1,1][1]*k[7][7][1]+RC[1][1,1][2]*Mod(k[7][7][2],y^2-d))*x1+
         (RC[1][1,2][1]*k[7][7][1]+RC[1][1,2][2]*Mod(k[7][7][2],y^2-d))*x2;
    z2 = (RC[1][2,1][1]*k[7][7][1]+RC[1][2,1][2]*Mod(k[7][7][2],y^2-d))*x1+
         (RC[1][2,2][1]*k[7][7][1]+RC[1][2,2][2]*Mod(k[7][7][2],y^2-d))*x2;
    F1 = bnfisprincipal(k,RC[2][1])[2];
    f1 = F1[1]*k[7][7][1]+F1[2]*Mod(k[7][7][2],y^2-d);
    F2 = bnfisprincipal(k,RC[2][2])[2];
    f2 = F2[1]*k[7][7][1]+F2[2]*Mod(k[7][7][2],y^2-d);
    ilist[i+1] = (z1*f1)/(z2*f2);
     )
}
```

```
%% Check that imag(ilist[i])>0 and imag(sigma(ilist[i])))>0
%% and set them equal to (z1,z2)
{z1s=vector(h,j,0);
 z2s=vector(h,j,0);
 for(i=1,h,
     zs=vector(2,j,0); r=1;
     for(j=1,4,s=lift(subst(ilist[i],x,nfgaloisconj(K)[j]));
               s1=subst(s,x,K[7][6][1]);
               if(imag(s1) > 0,
                  zs[r]=s; r=r+1;
                );
         );
     z1s[i]= subst(lift(subst(zs[1],x,K[7][6][1])),y,sqrt(d));
     z2s[i]= subst(lift(subst(zs[2],x,K[7][6][1])),y,sqrt(d));
     );
}
**************Hilbert functions********************

Kappa(k)= ((2*Pi)^(2*k)*sqrt(5))/(factorial(k-1)^2
          *(5^k)*zetak(zetakinit(x^2-5),k));
d=5;
L=nfinit(x^2-d);
abound = 20;

bt(k,a,b) =
{normab = a^2+a*b-b^2;
t= a+b*((1-Mod(x,x^2-d))/2);
PP=idealfactor(L,t);
m=matsize(PP);
divnorm=divisors(normab);
l=length(divnorm);
B=1;
for(i=2,l,
    F=factor(divnorm[i]);
    numfactor=matsize(F)[1];
    S=1;
    for(j=1,numfactor,
        if(kronecker(F[j,1],d)==-1, if(Mod(F[j,2],2)==1, S=0));
        if(kronecker(F[j,1],d)==1,
       whichideals=vector(2,i,0); r=1;
       for(n=1,m[1], if(PP[n,1][1]==F[j,1], whichideals[r]=n; r=r+1) );
       if(whichideals[2]==0, multiplier=1,
          i1=PP[whichideals[1],2]; i2=PP[whichideals[2],2]; I2=min(i1,i2);
          if(F[j,2]<I2, multiplier=F[j,2]+1,
         if(F[j,2]>max(i1,i2), multiplier=(i1+i2-F[j,2])+1,
               multiplier=I2+1
            );
          );
          );
        S=S*(multiplier);
         );
        );
    B=B + S*divnorm[i]^(k-1);
    );
(Kappa(k)*B)
}

{G(k) = sum(a=1,abound,
```

```
            sum(b=0, floor(((1+sqrt(5))/2)*a), bt(k,a,b)*q1^a*q2^b,
                sum(b=1, floor(-((1-sqrt(5))/2)*a),bt(k,a,-b)*q1^a*q2^(-b))
            )
       ,1)
}

J1=vector(h,i,0); J2=vector(h,i,0);
{for(i=1,h, z1=z1s[i]; z2=z2s[i];
Gk(k,z1,z2)=subst(subst(G(k),q1,
exp(2*Pi*I*((1+sqrt(5))*z1/(2*sqrt(5))-(1-sqrt(5))*z2/(2*sqrt(5)))))),q2,
exp(2*Pi*I*(z2-z1)/(sqrt(5))));
G2=Gk(2,z1,z2);
G4=Gk(4,z1,z2);
G6=Gk(6,z1,z2);
G10=Gk(10,z1,z2);
theta6 = -67*(2^5*3^3*5^2)^(-1)*(G6-G2*G4);
theta10 =2^(-10)*3^(-5)*5^(-5)*7^(-1)*(412751*G10-5*67*2293*G4*G6
+ 2^2*3*7*4231*G4^2*G2);
J1[i] = theta6/(G2^3);
J2[i] = (G2^5)/theta10;
    );
}

%% Gundlach class polynomials:
P1 = prod(i=1,h,X-J1[i]);
P2 = prod(i=1,h,X-J2[i]);
```

A.2. Mestre's algorithm for genus 2 curves

We recall Mestre's algorithm to generate a genus 2 curve with given Igusa invariants. Let k be a field of characteristic not equal to 2. By Section 2.2, a genus 2 curve X over k is determined by its Igusa invariants $j_i(X) \in F$. Conversely, however, given $j_i \in k$, one might not always find a genus 2 curve X defined over k such that $j_i(X) = j_i$ although such a curve X exists over a finite extension of k. This is due to the subtle difference between the definition field of X as a point in $\mathcal{C}_2(k)$ (field of moduli) and the definition field of X as a curve (the 'minimal' field where X has a model). Mestre discovered an algorithm to tell whether such a curve X over k exists and how to construct a model of X over k if it exists. We keep the notation from Section 2.2. Following [Me, p. 332 and p. 319] (his A'–D' are our A–D, and his A–D have a different meaning. We use his definition and solve the equations in [Me, p. 319] to get the formula for x, y, z in terms of Igusa's A, B, C, and D as follows), set

$$x = \frac{8}{225}\left(1 + 20\frac{B}{A^2}\right),$$

$$y = \frac{16}{3375}\left(1 + 80\frac{B}{A^2} - 600\frac{C}{A^3}\right),$$

$$z = \frac{-64}{253125}\left(-108 \cdot 10^5\frac{D}{A^5} - 9 - 700\frac{B}{A^2} - 3600\frac{C}{A^3} + 12400\frac{B^2}{A^4} - 48 \cdot 10^3\frac{BC}{A^5}\right).$$

In terms of the Igusa invariants, one has

$$x = \frac{8}{225}\left(1 + 20\frac{j_2}{j_1}\right),$$

$$y = \frac{16}{3375}\left(1 + 80\frac{j_2}{j_1} - 600\frac{j_3}{j_1}\right),$$

$$z = \frac{-64}{253125}\left(-108\cdot 10^5\frac{1}{j_1} - 9 - 700\frac{j_2}{j_1} - 3600\frac{j_3}{j_1} + 12400\left(\frac{j_2}{j_1}\right)^2 - 48\cdot 10^3\frac{j_2}{j_1}\frac{j_3}{j_1}\right). \tag{A.1}$$

Let $L \in \mathbb{P}^2$ be Mestre's conic given by the equation $v^t L v = 0$ with variables $v = (v_1, v_2, v_3)^t$ and

$$L = \begin{pmatrix} x+6y & 6x^2+2y & 2z \\ 6x^2+2y & 2z & 9x^3+4xy+6y^2 \\ 2z & 9x^3+4xy+6y^2 & 6x^2y_2y^2+3xz \end{pmatrix}. \tag{A.2}$$

Let M be Mestre's cubic curve in $\mathbb{P}^2$ given by

$$\sum_{1\leqslant i,j,k\leqslant 3} c_{ijk} v_1 v_2 v_3 = 0. \tag{A.3}$$

Here c_{ijk} are given by

$$\begin{aligned}
c_{111} &= 36xy - 2y - 12z,\\
c_{112} &= -18x^3 - 12xy - 36y^2 - 2z,\\
c_{113} &= -9x^3 - 36x^2y - 4xy - 6xz - 18y^2,\\
c_{122} &= c_{113},\\
c_{123} &= -27x^4 - 18x^2y - 18xy^2 - 3xz - 2y^2 - 12yz,\\
c_{133} &= -\frac{27}{2}x^4 - 72x^3y - 6x^2y - 9x^2z - 39xy^2 - 36y^3 - 2yz,\\
c_{222} &= -81x^4 - 54x^2y - 18xy^2 - 8y^2 + 6yz,\\
c_{223} &= 9x^3y - 27x^2z + 6xy^218y^3 - 8yz,\\
c_{233} &= -\frac{81}{2}x^5 - 27x^3y - 9x^2y^2 - 4xy^2 + 3xyz - 6z^2,\\
c_{333} &= \frac{81}{2}x^4y - \frac{81}{2}x^3z + 27x^2y^2 + 9xy^3 - 18xyz + 4y^3 - 30y^2z.
\end{aligned}$$

The conic curve L is given in [Me, pp. 321, 332] and the cubic curve M is given in [Me, p. 321] together with explicit formulae for a_{ijk} in [Me, p. 318] (which relate to c_{ijk} by the remark in [Me, p. 321]). Translating his parameters to our parameters gives the above explicit formula. Alternatively, one can use the formulae in [vW, p. 314] for L and M, which use the same parameters as in this paper. To get our equation from his, simply write the curve M in terms of v_i instead of his x_i, and then dividing the resulting equation by (his notation)

$$2^{67}\cdot 3^{22}\cdot 5^{23} I_2^{23} I_{10}^{12}.$$

As noted in [Me], c_{ijk} are absolute invariants while a_{ijk} are not. Mestre proved in [Me] that the genus 2 curve X with Igusa invariants $j_i(X) = j_i$ has a model over a field k of characteristic not equal to 2 if and only if $L(k)$ is not empty. It can be rephrased as follows.

Proposition A.1. *Let the notation be as above. Then the following are equivalent.*

(1) *X has a model over k.*

(2) *The conic curve L has a rational point over k.*
(3) *The ternary quadratic form Q associated to the matrix L represents* 0 *in k.*
(4) *Let $V = k^3$ be endowed with the quadratic form $Q(v) = v^t L v$, and let $B = C^+(V)$ be the associated even Clifford algebra, which is a quaternion algebra over k. Then B is isomorphic to the matrix algebra $M_2(k)$ over k.*

Proof. As mentioned above, Mestre proves the equivalence of (1) and (2). (3) is just reformulation of (2). The equivalence between (3) and (4) is a well-known classical fact in algebra. □

Suppose that the conic L has a rational point over k. Using this point, we can easily rewrite it as a parametric function

$$v_i = f_i(t),$$

for some quadratic polynomial of t. In particular this gives an explicit isomorphism between L and $\mathbb{P}^1$ over k. Plug these equations into the equation for the cubic curve M, we obtain a polynomial equation of t of degree 6 – call it $f(t) = 0$. Then the genus 2 curve C is given by (inhomogeneous) [Me, p. 321].

$$X : s^2 = f(t). \tag{A.4}$$

References

[BY] B.H. Bruinier, T.H. Yang, CM-values of Hilbert modular functions, Invent. Math. 163 (2006) 229–288.
[EL] K. Eisenträger, K. Lauter, A CRT algorithm for constructing genus 2 curves over finite fields, SMF Sém. Congrès 21 (2009) 161–176, http://arxiv.org/abs/math/0405305.
[GH] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, A. Weng, The 2-adic CM method for genus 2 curves with applications to cryptography, in: Asiacrypt, 2006, Shanghai, in: Lecture Notes in Comput. Sci., vol. 4284, Springer-Verlag, 2006, pp. 114–129.
[Ge] G. van der Geer, Hilbert Modular Surfaces, Springer-Verlag, 1988.
[Gu] K.-B. Gundlach, Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}(\sqrt{5})$, Math. Ann. 152 (1963) 226–256.
[Ho] E.W. Howe, Principally polarized ordinary abelian varieties over finite fields, Trans. Amer. Math. Soc. 347 (7) (1995) 2361–2401.
[HNR] E.W. Howe, E. Nart, C. Ritzenthaler, Jacobians in isogeny classes of abelian surfaces over finite fields, Ann. Inst. Fourier (Grenoble) 59 (2009) 239–289.
[Ig1] J.-I. Igusa, Arithmetic variety of moduli for genus two, Ann. Math. 72 (1960) 612–649.
[Ig2] J.-I. Igusa, On Siegel modular forms of genus 2, Amer. J. Math. 84 (1962) 175–200.
[Ig3] J.-I. Igusa, Modular forms and projective invariants, Amer. J. Math. 89 (1967) 817–855.
[Ig4] J.-I. Igusa, On the ring of modular forms of degree two over $\mathbb{Z}$, Amer. J. Math. 101 (1979) 149–183.
[Ko] D. Kohel, Igusa CM invariants database, http://echidna.maths.usyd.edu.au/kohel/.
[Me] J.-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, in: Effective Methods in Algebraic Geometry, Castiglioncello, 1990, in: Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334.
[Nag] S. Nagaoka, On the ring of Hilbert modular forms over $\mathbb{Z}$, J. Math. Soc. Japan 35 (1983) 589–608.
[Re] H.L. Resnikoff, On the Graded Ring of Hilbert modular forms associated with $\mathbb{Q}(\sqrt{5})$, Math. Ann. 208 (1974) 161–170.
[Sp] A.-M. Spallek, Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen, PhD thesis, Universität Gesamthochschule Essen, 1994.
[St] M. Streng, Computing Igusa Class Polynomials, preprint, http://arxiv.org/abs/0903.4766, 2009.
[vW] P. van Wamelen, Examples of genus two CM curves defined over the rationals, Math. Comp. 68 (225) (1999) 307–320.
[We] A. Weng, Constructing hyperelliptic curves of genus 2 suitable for cryptography, Math. Comp. 72 (241) (2003) 435–458.
[Ya1] T.H. Yang, An arithmetic intersection formula on Hilbert modular surfaces, Amer. J. Math., pp. 35, in press.
[Ya2] T.H. Yang, Arithmetic intersection on a hilbert modular surface and faltings' height, preprint, 2007, pp. 44.